Code No: F-13925/N/BL/AICTE

# FACULTY OF ENGINEERING

B.E. (CSE) VI –Semester (AICTE) (Main & Backlog) (New) Examinations,
August/September 2024

Subject: Cryptography and Network Security

Time: 3 Hours Max. Marks: 70

Note: (i) First question is compulsory and answer any four questions from the remaining six questions. Each question carries 14 Marks.
(ii) Answer to each question must be written at one place only and in the same order as they occur in the question paper.
(iii) Missing data, if any, may be suitably assumed.

1. a) Define Cryptanalysis?
b) Explain various types of Cryptanalytic attacks.
c) What is S-Box, explain with a neat diagram.
d) What are the differences between stream cipher and block cipher.
e) What are the two approaches of Digital Signature?
f) List out the properties of hash function.
g) Write the applications of IPSec.

2. a) List and briefly define categories of Security Services & Mechanisms.
b) Explain the different types attacks with examples.

3. a) Briefly explain about single round function of AES..
b) Elucidate Data Encryption Standard with block Diagram?

4. a) Briefly discuss about Diffie-Hellman Key Exchange algorithm?
b) Perform decryption and encryption using RSA algorithm with p=3,q=11,e=7,N=5.

5. a) What is digital signature? Explain RSA Digital Signature Scheme.
b) Explain SHA-512 block diagram and compression function.

6. a) Explain S/MIME protocol.
b) Explain SSL protocol with neat diagram.

7. a) Explain the Chinese remainders theorem.
b) Compare and contrast the difference between symmetric key and asymmetric key cryptography.

**